

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

UNITED STATES OF AMERICA

v.

RICHARD BARNETT

Case No. 17-CR-00676

Judge John Robert Blakey

MEMORANDUM OPINION AND ORDER

On February 7, 2018, a grand jury indicted Defendant on one count of child sexual exploitation in violation of 18 U.S.C. § 2251(a). [36]. A superseding indictment on May 25, 2022 added additional child sexual exploitation counts, as well as one count of transmitting threats to kidnap or injure a person in violation of 18 U.S.C. § 875(c); one count of transmitting threats to injure a person's reputation in violation of 18 U.S.C. § 875(d); and two counts of possessing child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). [137].

On May 6, 2021, Defendant moved to quash certain search warrants and suppress evidence seized pursuant to their execution, including subsequent statements he made to FBI agents. [110]. First, Defendant argues that a Louisiana state court issued an invalid warrant for his "Musical.ly" social media account because the warrant application did not establish probable cause for its issuance. This, he argues, also invalidates subsequent federal search warrants as fruits of the poisonous tree pursuant to *Wong Sun v. United States*, 371 U.S. 471 (1963).

Second, relying on *Carpenter v. United States*, 138 S. Ct. 2206 (2018), Defendant argues that the FBI also unlawfully obtained the dynamic IP address

records for his mobile phone without a warrant. [133]. He insists that the FBI “predicated its entire investigation” upon this dynamic IP address information, which provides another reason to quash the federal search warrants and suppress any evidence derived from them. [110] at 1, 6; [141].

On July 6, 2022, and August 8, 2022, the Court held an evidentiary hearing on Defendant’s motion [110]. At the hearing, the Government presented testimony from FBI Special Agent Shannon McDaniel, the current FBI case agent. Defendant chose not to call any witnesses, but both parties introduced, by agreement, documentary evidence and, on August 22, 2022, they submitted a joint factual stipulation, [145].¹

On December 8, 2022, [146], the Court orally denied Defendant’s motion [110]. Based upon the record, the Court now issues its specific factual findings and its resulting conclusions of law.

I. Factual Findings

A. Florida Investigation

On May 8, 2017, a Florida elementary school complained to Jacksonville Florida Sheriff’s Office that, on May 6 and 7, 2017, several female minors had

¹ In addition to the testimony of FBI Special Agent McDaniel, the Government offered seven exhibits, MTS1–MTS7, to which Defendant agreed both as to authenticity and the truth of the facts contained therein. Redacted versions of five of these exhibits appear on the docket—[112-1] (Ex. MTS1A); [112-2] (Ex. MTS2A); [125-2] (Ex. MTS4A); [125-1] (Ex. MTS5A); and [125-3] (Ex. MTS6). The Government did not file MTS3 (Ouachita Parish, Louisiana Sheriff’s Office Investigation Report) or MTS7 (Subpoena and Return for May 10, 2017 subpoena issued by the State Attorney of Fourth Judicial Circuit of Florida to Musical.ly Inc.), but provided hard copies to the Court and Defendant. Defendant also offered six exhibits, to which the Government agreed both as to authenticity and the truth of the facts contained therein. Five of these exhibits appear on the docket—[129-1] (Barnett Ex. 1); [30] (Barnett Ex. 2); [20] (Barnett Ex. 3); [24] (Barnett Ex. 4); and [27] (Barnett Ex. 5). The docket only includes a partial copy of Barnett Exhibit 6 (July 25, 2017 administrative subpoena to Verizon for the mobile device records, including IP address information), *see* [136-1], but Defendant provided a complete copy to the Court and Government.

received obscene chat messages on the internet video-sharing and messaging application, Musical.ly. *See* Ex. MTS4 at 1–2. Investigators interviewed the minors and their parents who reported that an account—which reportedly used screen names “david banks” and “davidbank1014,” and claimed to be a 13-year-old boy—sent the minors sexually explicit messages, tried to persuade them to put their hands down their pants, and asked that they record and send videos of their faces while they masturbated. *Id.* at 1–2, 5–7. The account’s user also threatened to find and kidnap some of the minors and to “kidnap, rape and kill” them if they told anyone about him. *Id.* at 6–7. One of the minors gave the Sheriff’s Office screenshots of some of the chats. *Id.* at 7. One parent also reported that she created a fake Musical.ly account posing as a 13-year-old, and the alleged offending account began to follow her account. *Id.*

In response, Jacksonville Sheriff’s Office subpoenaed Musical.ly for subscriber information associated with “davidbank1014” and “david banks.” *Id.* at 7–8; MTS7. In response, Musical.ly asked for “a ‘screen shot’ of the suspect’s profile to complete” the request, which the Sheriff’s Office obtained from one of the victims and then sent to Musical.ly. MTS4 at 9. In response, Musical.ly returned the mobile telephone number for the account, and the mobile device type associated with the username “davidbanks1014.” MTS7. Musical.ly’s response also indicated that the account was created on April 22, 2017 using the Internet Protocol (“IP”) address 70.175.173.104. *Id.* As agreed by the parties, an “IP address” is a unique series of numbers that a

device uses to connect to the internet, and when a device accesses a website, the device's IP address tells the website where to route the website data. [145] ¶ 1.

Next, the Sheriff's Office followed up on the subpoena returns. First, the Sheriff's Office used databases to look up the mobile telephone number from the Musical.ly subpoena results; and investigation of this directory connected the number to the name Richard D. Barnett with an Aurora, Illinois address. MTS4 at 8. The Sheriff's Office, through the State's Attorney's Office, also subpoenaed Verizon for the subscriber information associated with the mobile device, and Verizon sent back the name Richard D. Barnett, but with an address in Rochester, New York. *Id.* The Sheriff's Office also compiled a photo array that included the suspect's photo (Defendant), since one of the minors had reported that the account sent her a video showing the suspect. *Id.* at 8–9. That minor reviewed the photo array but said “they all kind of look like him.” *Id.* at 9.

Because Verizon identified an address in Rochester, New York, the Sheriff's Office referred the matter to the FBI Field Office in Buffalo, New York. MTS5 at 1. There, FBI Agents subpoenaed Cox Communications for information associated with the IP address 70.175.173.104 on April 22, 2017, the day the davidbanks1014 account was created. *Id.* at 2. Cox Communications reported that an apartment building in Oklahoma City, Oklahoma had used the IP address on that date. *Id.*

Next, the FBI Agents subpoenaed Verizon for the IP address logs for the mobile device number associated with the Musical.ly account for three relevant dates: May 6–7, 2017 (the dates the victims alleged the account messaged them) and July 24,

2017 (a date close to the subpoena request).² *Id.* at 2; Barnett Ex. 6. Verizon returned the requested IP addresses linked to the mobile device; an FBI Agent, using a publicly accessible IP geolocation website, linked the IP addresses to the general Chicago Illinois area. MTS5 at 2.

The FBI agent also found a public Facebook account for a “rickn.barnett” that showed the user was from Rochester, New York; had started working for the Federal Aviation Administration (“FAA”) in February 2017; and currently lived in Aurora, Illinois. *Id.* at 3. An Accurint.com public record search for “Richard Barnett” also listed a possible address in Aurora, Illinois. *Id.*

Based upon this open-source information, the FBI Buffalo Field Office referred the case to the FBI Chicago Field Office on August 30, 2017. *Id.*

B. Louisiana Investigation

Independently, on June 4, 2017, the father of a nine-year-old girl (“Victim A”) in Louisiana complained to the Ouachita Parish, Louisiana Sheriff’s Office that someone with the screen name “@davidbanks1014” or “David Banks” had sent her sexually inappropriate and harassing messages through Musical.ly. *See* MTS1. Victim A told sheriff’s deputies that the individual told her to record herself touching her leg; when she sent a video of herself touching her thigh, the individual responded, “no touch your candy,” and then instructed her to put her hand down her pants and

² This is the subpoena that Defendant, relying on *Carpenter*, 138 S. Ct. at 2206, argues violated his Fourth Amendment rights. [133]; [141]. The FBI issued this subpoena pursuant to 18 U.S.C. § 3486, which authorizes certain government agents to issue administrative subpoenas when investigating certain crimes, including federal offenses involving sexual exploitation or child abuse. *See* Barnett Ex. 6 at 2.

rub. *Id.* at 2. Victim A also told deputies that, after that exchange, the account logged onto Musical.ly anytime she logged on and started following some of her friends' Musical.ly accounts. *Id.* Victim A's father told deputies that he and his wife created a fake account on Musical.ly to find out additional information about the offending account, but "the family was unsuccessful." *Id.*

Based upon this citizen complaint, on July 19, 2017, Ouachita Parish Senior Investigator James W. Humphrey presented a search warrant application to Judge Wilson Rambo of the Fourth Judicial District Court, in Ouachita Parish, Monroe, Louisiana to secure Musical.ly's records for the "@davidbanks1014" account, including subscriber information, chat logs, and IP session logs (hereinafter, "Louisiana Search Warrant"). MTS2. In support of probable cause for the warrant, Senior Investigator Humphrey submitted a statement, which he swore to under oath before Judge Rambo, that summarized the information that Victim A and her father reported, including the parents' unsuccessfully effort to "secure information about the suspect" by creating a fake Musical.ly account. *Id.* at 4. Judge Rambo reviewed and then signed the warrant that same day. *Id.* at 2, 5.

On July 20, 2017, Musical.ly returned records for the @davidbanks1014 account. *Id.* at 6. The records showed that the user created the account on April 22, 2017, and included the mobile number, type of cellular device, and the IP address used to create the account. Barnett Ex. 1 ¶ 24. The records also included the account's stored chat logs and partial IP address session logs. *Id.* ¶¶ 24–25. While the chat logs did not include the messages with Victim A, they contained other chats

with additional female minors about engaging in sexually explicit activity. *Id.* ¶¶ 26–39. In some instances, the minors and @davidbanks1014 exchanged images of their genitalia. *Id.* Also, the target account had sent one minor, Victim C, violent and threatening texts, including threats to find, rape, and kill her; an image of a handgun; and threats to circulate revealing images of her if she did not send a video of herself masturbating. *Id.*

After receiving the Louisiana Search Warrant results, the Ouachita Sheriff's Office conducted additional investigative steps, including sending an administrative request to Comcast Cable Communications for the subscriber information for one of the IP addresses. *Id.* ¶ 39. Comcast's records linked the IP address to Defendant and to Defendant's Aurora home. *Id.* The registered phone number in Comcast's business records also matched the phone number linked to the @davidbanks1014 account. *Id.* ¶ 39.

FBI Agent McDaniel—the current case agent on the case—testified that, based upon this link to Aurora, the Ouachita Sheriff's Office referred the Louisiana Investigation to the FBI's Chicago office on or about August 28, 2017.

C. FBI Chicago Office's Investigation

In September 2017, armed with information from both the Jacksonville and Louisiana investigations, Special Agent Kimberly Castro of the FBI Chicago Field Office issued an updated administrative records request to Comcast for the same IP address on which the Ouachita Sheriff subpoenaed records. The return showed that the IP address remained linked to Defendant's Aurora home as of September 4, 2017.

Barnett Ex. 1 ¶ 41. Because the Jacksonville Investigation found that Defendant may work for the FAA, Agent Castro also spoke to the FAA, which confirmed that Defendant worked at a facility in Des Plaines, Illinois; he had listed the Aurora address as his home address; and his phone number matched the one linked to the @davidbanks1014 Musical.ly account. *Id.* ¶ 42. The FAA also confirmed that Defendant had attended training in Oklahoma City from March 27–May 5, 2017 and, during that time, he resided at the apartment complex linked to the IP address used to create @davidbanks1014 account on April 22, 2017. *Id.* ¶ 43. Agent Castro also contacted the Post Office, which confirmed that Defendant, and only Defendant, received mail at the Aurora address; and she also searched Secretary of State records from October 4, 2017, which confirmed Defendant’s address in Aurora. *Id.* ¶¶ 46–47.

On October 13, 2017, Agent Castro applied for a search warrant for Defendant’s Aurora home, providing an affidavit that detailed the information that it received from both the Jacksonville Investigation and Louisiana Investigation, as well as the information Agent Castro gathered in September and early October. Barnett Ex. 1. United States Magistrate Judge Maria Valdez reviewed the application and issued the warrant, *id.*, which the agents executed on October 16, 2017, seizing, among other things, a computer containing child pornography and the phone tied to the number associated with the @davidbanks1014 Musical.ly account. Barnett Ex. 2 ¶¶ 7–10.

During the search, agents also interviewed Defendant, who admitted that he had multiple Musical.ly usernames incorporating “davidbanks”; used the account

@davidbanks1014; had communicated with female minors through his Musical.ly accounts; and had exchanged nude photos with some of those minors. *Id.* ¶ 8. Defendant also admitted that he possessed child pornography videos in a DropBox account to which he occasionally granted others access. *Id.*

Following the search, federal agents arrested Defendant for producing and transporting child pornography. *Id.* ¶ 9. On December 6, 2017, Agent Castro also obtained a search warrant to seize electronic data from DropBox, Instagram, Facebook, and Musical.ly accounts associated with Defendant. Barnett Exs. 2–5.

On February 7, 2018, the grand jury indicted Defendant for child sexual exploitation in violation of 18 U.S.C. 2251(a) and charged him, in a superseding indictment issued May 25, 2022, with additional child sexual exploitation counts, as well as one count of transmitting threats to kidnap or injure a person in violation of 18 U.S.C. § 875(c); one count of transmitting threats to injure a person's reputation in violation of 18 U.S.C. § 875(d); and two counts of possessing child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). [137]. [36], [137].

II. Analysis

Defendant seeks to quash the search warrants issued in this case, and to suppress evidence seized pursuant to those warrants, based upon two alleged Fourth Amendment violations. [110], [133].

First, he argues that this Court must quash the Louisiana Search Warrant and suppress the evidence obtained from it because the warrant application did not support a probable cause finding. [110]. Defendant maintains that the lack of

probable cause also invalidates, in turn, the federal search warrants issued for his Aurora home and other online accounts because those Chicago warrant applications relied in part upon information derived from the Louisiana Search Warrant. *Id.* In other words, he argues, the federal search warrants and the evidence obtained therefrom constitute fruits of the poisonous tree. *See Wong Sun*, 371 U.S. at 471.

Second, Defendant argues that the FBI Buffalo Field Office violated his Fourth Amendment rights when it obtained the dynamic IP address records for his mobile phone from Verizon through an administrative subpoena. *See* [133]; Barnett Ex. 6. He claims that the FBI “predicated its entire investigation” on this dynamic IP address information and relied upon in part it “to provide probable cause for” the Aurora home search warrant. [133] at 1, 6. This, he argues, provides the second basis to quash the Aurora home search warrant, as well as the subsequent search warrants, and suppress any evidence derived therefrom. *Id.*; [141].

The Court considers both alleged constitutional violations in turn.

A. Suppression of the Louisiana Search Warrant

As discussed above, the Louisiana Search Warrant application relied upon Victim A and her father’s statements to Ouachita Sheriff’s Office investigators. Even though a judge reviewed and signed the warrant, Defendant argues that Victim A’s allegations lacked reliability due to her age and because they remained uncorroborated. [110] at 5–6. He also argues that the application’s short summary of Victim A’s claims lacks certain details and therefore is patently insufficient for any probable cause finding. *Id.* The sworn statement does not, for example, include the

exact dates when Victim A allegedly received the messages from @davidbanks1014; nor does it explain exactly what the Musical.ly application is, how it works, or whether it stores users' messages or other information. *Id.* And although the warrant application stated that Victim A claimed that the @davidbanks1014 account logged on whenever she logged on and that it had started following her friends' Musical.ly accounts, Defendant complains that the sworn statement does not indicate whether any officers attempted to talk to Victim A's friends or otherwise corroborate this information. Likewise, Defendant argues, the warrant application acknowledges that Victim A's parents created a fake Musical.ly account but could not secure additional information about the offender. *Id.*

In response, the Government acknowledges that the Louisiana Warrant application provided less factual detail than typical search warrant applications in this district. [112] at 10. It argues, however, that the Louisiana warrant application provided sufficient probable cause under the requisite constitutional standard set out in *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

Second, the Government contends that, even in the absence of probable cause, suppression remains unwarranted pursuant to the good-faith exception under *United States v. Leon*, 468 U.S. 897 (1984). [112] at 7–13; *see also Davis v. United States*, 564 U.S. 229, 241 (2011); *United States v. Berrios*, 990 F.3d 528 532 (7th Cir. 2021).

Third, it argues that, even if the Court suppresses the Louisiana Search Warrant itself, the Court should not quash the federal search warrants, or suppress the evidence obtained therefrom, because the Chicago Field Office's investigation

remained sufficiently attenuated from the Louisiana investigation, citing *United States v. Conrad*, 673 F.3d 728, 732–33 (7th Cir. 2012). [112] at 14.

Fourth, the Government points to the inevitable discovery doctrine, arguing that, even without the Louisiana Search Warrant results, the Chicago Field Office could and would have obtained those records based upon information from the independent Jacksonville Investigation prior to seeking the federal warrants. [125].³

As explained below, Defendant’s motion to suppress the Louisiana Search Warrant, and other evidence as fruit of the poisonous tree, lacks merit.

1. Probable Cause Existed Under the Controlling Standard

The Fourth Amendment protects the people’s right “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” *United States v. Lewis*, 38 F.4th 527, 533–35 (7th Cir. 2022). If something qualifies as a search, then generally the Government must obtain a warrant supported by probable cause, unless an exception applies. *Id.* (citing *Lange v. California*, 141 S. Ct. 2011, 2017 (2021)). Probable cause for a search warrant, in turn, requires “a fair probability that contraband or evidence of a crime will be found in a particular place.” *United States v. Gibson*, 996 F.3d 451, 461 (7th Cir. 2021) (quoting *Gates*, 462 U.S. at 238).

³ The Government first raised inevitable discovery in a supplemental response filed after Defendant’s reply because it only belatedly learned that the FBI Buffalo Office independently referred the Jacksonville Investigation to the FBI Chicago Office. [125] at 2–4. The Government had previously believed in error (but in good faith) that the FBI learned of the Jacksonville Investigation through its investigation into the information it received from Louisiana. *Id.* Having given Defendant a full opportunity to respond to this theory, the Court considers the inevitable discovery doctrine as well.

In assessing probable cause, this Court “does not deal with hard certainties,” but rather “with probabilities.” *Gates*, 462 U.S. at 231 (quoting *United States v. Cortez*, 449 U.S. 411, 418 (1981)). Although probable cause requires “something more than a hunch,” it requires “only a substantial chance of criminal activity, not an actual showing of such activity.” *United States v. Schaafsma*, 318 F.3d 718, 722 (7th Cir. 2003); *see also Abbott v. Sangamon Cty., Ill.*, 705 F.3d 706, 714 (7th Cir. 2013). As a result, probable cause exists even though there “could have been innocent explanations” for the targeted activity, so long as “the inference of the criminal activity was reasonable.” *United States v. Gary*, 790 F.3d 704, 707–08 (7th Cir. 2015) (citing *United States v. Funches*, 327 F.3d 582, 587 (7th Cir. 2003)); *see also United States v. Burnside*, 588 F.3d 511, 518 (7th Cir. 2009) (holding that probable cause remains “a fluid concept” based upon “common-sense interpretations of reasonable police officers as to the totality of the circumstances known at the time the event occurred.” (quoting *United States v. Ellis*, 499 F.3d 686, 689 (7th Cir. 2007))).

The analysis must examine probable cause “from the perspective of what” the officers knew collectively “at the time” of the search or seizure, *Fox v. Hayes*, 600 F.3d 819, 832 (7th Cir. 2010), rather than engaging in some “post hoc determination,” *United States v. Reed*, 443 F.3d 600, 603 (7th Cir. 2006); *see also United States v. Howard*, 883 F.3d 703, 707 (7th Cir. 2018) (holding that, under the “collective knowledge” doctrine, the police officers who actually make an arrest or search “need not personally know all the facts that constitute probable cause if they reasonably are acting at the direction of another officer or police agency.”). It also must consider

the facts from “the standpoint of an objectively reasonable police officer,” although viewed “through the prism” of the officers’ “training and experience.” *Burnside*, 588 F.3d at 518. At all times, a court’s probable cause inquiry remains an objective one; the subjective motivations of the officers cannot invalidate a search or seizure otherwise supported by probable cause. *See Carmichael v. Vill. of Palatine, Ill.*, 605 F.3d 451, 457 (7th Cir. 2010).

Finally, a court must afford a prior judge’s probable cause finding “a strong presumption of correctness,” and will not disturb it so long as it finds “a substantial basis for concluding that probable cause existed.” *Gibson*, 996 F.3d at 461 (quoting *United States v. Sanchez-Jara*, 889 F.3d 418, 421 (7th Cir. 2018) and then *Gates*, 462 U.S. at 238–39).

Applying the *Gates* standard, the factual record here shows probable cause for issuing the Louisiana Search Warrant. As detailed above, the affiant-officer, under oath, related specific information that known citizen-complainants provided, including the first-hand information from the victim establishing a crime—the unlawful sexual solicitation of a minor (among other potential offenses). Specifically, it summarized how the father of the nine-year-old victim female personally complained to the Ouachita Parish Sheriff’s Office that someone with the screen name “@davidbanks1014” or “David Banks” had sent sexually inappropriate and harassing messages to the victim through the video-sharing app Musical.ly. *See* MTS1; MTS2. Further, the minor victim not only told her parents about the messages, but she provided her first-hand observations of the targeted account to the

Sheriff's investigator, including descriptions of how the individual using that account engaged in private criminal behavior by: (1) telling her to record herself touching her leg; (2) stating "no touch your candy" when the victim sent a video of herself only touching her thigh; and (3) instructing her to put her hand down her pants and rub. MTS1; MTS2. The victim also told deputies that, after that exchange, the account logged onto Musical.ly anytime she logged on, and that it started following some of her friends' Musical.ly accounts. MTS1; MTS2

Notwithstanding the victim's young age, a reasonable officer would have reason to find her account credible under the circumstances, including the details she offered about the offending messages and the account that sent them, as well as the corroborating statements from the victim's father. *See, e.g., Holmes v. Vill. of Hoffman Est.*, 511 F.3d 673, 680 (7th Cir. 2007) (holding that for probable cause an officer "may rely on information provided to him by the victim or by an eyewitness to the crime that the officer reasonably believes is telling the truth." (citing *Pasiewicz v. Lake Cty. Forest Preserve Dist.*, 270 F.3d 520, 524 (7th Cir. 2001) and *Gramenos v. Jewel Cos.*, 797 F.2d 432, 439 (7th Cir. 1986))); *Grimm v. Churchill*, 932 F.2d 674, 675 (7th Cir. 1991) (holding that "when an officer has 'received his information from some person—normally the putative victim or an eyewitness—who seems reasonable to believe is telling the truth,'" the officer "has probable cause." (quoting *Gramenos*, 797 F.2d at 439)); *Jenkins v. Keating*, 147 F.3d 577, 585 (7th Cir. 1998) ("So long as a reasonably credible witness or victim informs the police that someone has committed, or is committing, a crime, the officers have probable cause"); *Gerald M. v.*

Conneely, 858 F.2d 378, 381 (7th 1988); *Jones v. City of Chi.*, 856 F.2d 985, 994 (7th Cir.1988) (holding that identification given by a “lucid” victim would establish probable cause); *Sheik-Abdi v. McClellan*, 37 F.3d 1240, 1247 (7th Cir. 1994); *Bates v. Stevenson*, No. 93 C 1815, 1996 WL 327811, at *4 (N.D. Ill. June 12, 1996) (holding that since information came from “an ordinary citizen, his identification of [offender] carries a presumption of reliability”); *Huffman v. Grinnell*, 880 F. Supp. 1194, 1198 (N.D. Ill. 1995) (“Information supplied by an ordinary citizen” to the police “carries a presumption of reliability.”).⁴

Overall, this Court finds that probable cause existed for the issuance and execution of the Louisiana Search Warrant under the Fourth Amendment.

2. Good Faith Exception Applies

Even if the record lacked probable cause for the search warrant, this Court also finds that the good faith exception applies. The good faith exception permits admission of evidence obtained in violation of the Fourth Amendment “if the officers conducted the search in good-faith reliance on a warrant.” *United States v. Matthews*, 12 F.4th 647, 651 (7th Cir. 2021) (citing *Leon*, 468 U.S. at 922); *see also Davis*, 564

⁴ Even though the parents failed in their efforts to gather more information about the offending account by creating a fake Musical.ly account, this does not materially undermine the credibility of Victim A’s statements. Unlike anonymous tipsters, identified victim-witnesses remain subject to criminal and civil penalties for making false reports to the police, and their accounts otherwise bring with them an intrinsic presumption of reliability in assessing probable cause. Here, the officers had no cause to disbelieve the ordinary citizens who came to them for help; and, in any event, the officer disclosed their unsuccessful effort with the fake account in his sworn affidavit to Judge Rambo. Without doubt, the record still provides “a substantial basis for concluding that probable cause existed” notwithstanding this one setback. *See Gibson*, 996 F.3d at 461. In short, Judge Rambo’s finding warrants “a strong presumption of correctness” and this Court concurs with his finding of probable cause. *Id.*

U.S. at 238 (“But when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrent value of suppression is diminished, and exclusion cannot pay its way.” (internal quotations and citations omitted)). The Government bears the initial burden to establish an officer acted in good faith, but an “officer’s decision to obtain a warrant is *prima facie* evidence of his good faith.” *Matthews*, 12 F.4th at 653. That being the case here, Defendant bears the “heavy” burden “to rebut that presumption.” *Id.* (citing *Edmonds v. United States*, 899 F.3d 446, 453 (7th Cir. 2018)). As explained below, Defendant failed to rebut the Government’s showing of good-faith.

To meet this “heavy burden,” Defendant must establish one of four things: (1) the application’s affiant misled the issuing judge with information that “the affiant knew was false or would have known was false but for the affiant’s reckless disregard for the truth”; (2) the issuing judge “wholly abandoned his judicial role and instead acted as an adjunct law-enforcement officer”; (3) the affidavit so lacked “indicia of probable cause as to render official belief in its existence entirely unreasonable”; or (4) the warrant “was so facially deficient in particularizing its scope that the officers could not reasonably presume it was valid.” *United States v. Rees*, 957 F.3d 761, 771 (7th Cir. 2020) (quoting *Leon*, 468 U.S. at 923).

Defendant does not establish any these four alternatives. He offers nothing to suggest that the officer-affidavit knowingly or recklessly misled the issuing judge, nor does he argue that the warrant lacked a particularized scope. While he argues that

the affidavit remained barebones and lacked any “indicia of probable cause,” [122] at 6–7, the Court already discussed above why these arguments lack merit.

That leaves only the second alternative—that the issuing judge “wholly abandoned his judicial role.” Here, Defendant points to one fact—Judge Rambo signed the warrant purportedly one minute after the affiant-officer swore to the truth of his affidavit. [115] at 9. He argues that Judge Rambo could not have meaningfully reviewed the affidavit in that time, and instead acted as “a rubber stamp for the police.” *Id.* Not so.

Even if Judge Rambo signed the affidavit one minute after the affiant-officer swore to the truth of the affidavit, this does not show, or even suggest, that Judge Rambo only reviewed the warrant application or affidavit for one minute or that he otherwise “rubber stamped” the warrant application. To the contrary, based upon common practice, it remains far more likely that Judge Rambo reviewed the warrant application and, after reviewing it, the officer swore to the truth of the affidavit.

Defendant has not met his “heavy burden” to rebut the presumption of good faith. As such, the good-faith exception applies here even if there lacked probable cause to issue the Louisiana Search Warrant.

3. Inevitable Discovery Doctrine Applies

Finally, the inevitable discovery doctrine also dooms Defendant’s motion.⁵ Thus, even if the Louisiana Search Warrant application did not support a probable cause finding (which it did), the exclusion of evidence remains unwarranted.

⁵ Given this Court’s findings of fact and conclusions of law today, no need exists to address the Government’s third argument based upon an attenuation theory.

For this doctrine to apply, the Government must establish by a preponderance of the evidence “that the information ultimately or inevitably would have been discovered by lawful means.” *United States v. Alexander*, 573 F.3d 465, 477 (7th Cir. 2009) (quoting *Nix v. Williams*, 467 U.S. 431, 444 (1984)). To meet its burden, the Government must show two things: (1) “it had, or would have obtained, an independent, legal justification for conducting a search that would have led to the discovery of the evidence”; and (2) “it would have conducted a lawful search absent the challenged conduct.” *United States v. Rosario*, 5 F.4th 706, 713 (7th Cir. 2021) (quoting *United States v. Marrocco*, 578 F.3d 627, 637–38 (7th Cir. 2009)).

Here, inevitable discovery first requires the Government to establish that the FBI Chicago Field Office had independent probable cause for a search warrant for the same @davidbanks1014 Musical.ly records that the Louisiana Search Warrant produced. The Government has more than met its burden in this regard. As discussed above, the Jacksonville Sheriff’s Office received independent complaints from multiple minors (and their parents) that a Musical.ly account under the username “davidbanks” and “davidbank1014” sent the minors sexually explicit chat messages; solicited and, in some instances obtained, pornographic images of the children; and threatened to kidnap, rape and/or murder some of the minors.

Pursuant to *Gates*, 462 U.S. at 238, these victim-witnesses’ complaints established probable cause based upon the totality of the circumstances (even excluding what the Louisiana Search Warrant revealed). Despite Defendant’s objection to use of victim reports from minors, he offers no facts establishing how the

testimony of these known citizen witnesses was flawed, and instead the record confirms that the independent and similar reports from multiple minors (and their parents) remained credible. In addition to their own testimony, the minors gave corroborating information to the Sheriff's Office, including screenshots of chats and a screenshot of the account's profile page. A parent of one of the minors also reported that she created a fake Musical.ly account posing as a 13-year-old and the alleged offending account began to follow her. Further, based upon these citizen reports, the Jacksonville Sheriff's Office subpoenaed Musical.ly for subscriber information, and Musical.ly sent back additional corroborating account information for the Musical.ly username "davidbanks1014."⁶

Thereafter, the Jacksonville Sheriff's Office's detailed all this information in a report to the FBI Buffalo Field Office that then went to the FBI Chicago Field Office. Without doubt, the Jacksonville Investigation, including the minors' detailed accounts of the messages, establishes "a fair probability that contraband or evidence of a crime" would be found in the "davidbanks1014" Musical.ly records.⁷ *Gates*, 462

⁶ The investigator's report states that Musical.ly sent back account information for username "davisbanks1014." [125-2] at 9. Musical.ly's subpoena response, Ex. MTS7, confirms this was a typo and should have read "davidbanks1014." Based upon the record, this Court makes a finding of fact that the "typo" error was properly resolved, and thus, it is not material to the legal analysis of Defendant's motion.

⁷ Defendant disagrees, arguing that the Jacksonville minors' accounts could not establish probable cause for a warrant for the "davidbanks1014" account because the minors only complained about messages from "david banks" or "davidbank1014." [129] at 2. He argues that this is like seeking a warrant to search 123 Maine Street based upon information about 123 Main Street. *Id.* Not so. True, the Jacksonville Sheriff's Office's investigation report states that the minors complained about "david banks" or "davidbank1014" Musical.ly accounts. But even if this left an initial ambiguity about the alleged offender's username, the officer later obtained an account profile "screen shot" from one minor after Musical.ly requested clarification on the account name. And, after Musical.ly received that screen shot, it provided results for the corresponding account: "davidbanks1014." Ex. MTS7. Defendant argues that the FBI never saw a copy of this "screen shot" so one cannot know what it contained or draw any conclusions from it. Again, not so. The Jacksonville Sheriff's Office

U.S. at 238. Accordingly, the Government has met its burden as to the first prong of the inevitable discovery doctrine.

Next, the Government must establish by a preponderance of the evidence that “it would have conducted a lawful search absent the challenged conduct.” *Alexander*, 573 F.3d at 477. To meet its burden, the Government offered a sworn affidavit and the live testimony of FBI Special Agent Shannon K. McDaniel (the current case agent who also assisted in executing the federal search warrant of Defendant’s Aurora residence in October 2017). MTS6. Agent McDaniel has worked for the FBI since 2001 and in the FBI’s Chicago Field Office since 2006. *Id.* ¶ 1. Since 2005, she has primarily investigated federal criminal violations relating to child pornography and child exploitation, handling approximately twelve to fifteen cases at any given time, and assisting in executing at least twelve search warrants per year. She also testified that every child exploitation case she has investigated involved targets who communicated with minors over the internet.

Agent McDaniel stated in her affidavit and at the evidentiary hearing that, based upon her experience and training, she understands the policies and procedures of the FBI’s Chicago Field Office relating to these types of investigations and prosecutions. *Id.* ¶ 3. She also confirmed that she reviewed the lead and records from

investigation report, which the FBI received and reviewed, states that a Musical.ly representative “made contact with me and stated that he needed a ‘screen shot’ of the suspect’s profile to complete my request. I made contact with [one of the minors] and she sent me the requested information.” [125-2] at 9. Next, it states that, based upon this “screen shot,” Musical.ly sent back information on the “@davidbanks104” account. *Id.* Further, it notes that the officer placed into the Property and Evidence Facility a “Screen Shot of Suspect Profile.” *Id.* at 10. Considering the totality of these circumstances, this Court draws the reasonable inference, consistent with the conclusions of the officers and agents, that the “davidbanks1014” account sent the illicit messages to the minors.

the FBI's Buffalo Field Office, which included the Jacksonville Sheriff's Office investigation report. She testified that, if the FBI Chicago Field Office had not gotten the "davidbanks1014" chat log records from the Louisiana Investigation, the Chicago office still would have sought a federal search warrant for those records as part of its standard investigative procedure based upon the information from the Jacksonville Sheriff's Office and the FBI Buffalo Field Office. *Id.* ¶ 7. She explained that, because the minors in Jacksonville had reported that the "perpetrator was targeting minor females and had expressed a willingness to engage in extreme and fatal violence toward those victims, the case would have received immediate and serious attention from the Chicago Field Office." *Id.* ¶ 7b.

She also testified that the FBI Chicago Field Office would have obtained those Musical.ly chat logs before attempting to approach the suspect or search his home. In support, she explained that, when a case involves child sexual exploitation through social media, the FBI Chicago Field Office has a standard and regular practice "to secure electronic evidence from social media sites before making an overt approach to the primary suspect" because individuals often take steps to destroy such evidence if they learn about the FBI's interest in them. *Id.* ¶ 7c.

The Seventh Circuit has long held that the inevitable discovery doctrine rule applies "where investigating officers undoubtedly would have followed routine, established steps resulting in the issuance of a warrant." *United States v. Pelletier*, 700 F.3d 1109, 1117 (7th Cir. 2012) (quoting *Marrocco*, 578 F.3d at 639–40); *see also United States v. Buchanan*, 910 F.2d 1571, 1573 (7th Cir. 1990) (holding that,

pursuant to “proper and predictable police investigatory procedures,” police would have inevitably sought a warrant to search a room because “it would have been foolish not to want to look for the gun there.”).

Agent McDaniel’s sworn testimony establishes just that.⁸ Namely, her extensive experience investigating child exploitation, generally, and in the FBI Chicago Field Office, specifically, supports her understanding of FBI Chicago Field Office practices and procedures with respect to child exploitation cases like this one. Thus, her testimony establishes by a preponderance of the evidence that the FBI would have sought a search warrant for the “@davidbanks1014” Musical.ly records based upon the information from the Jacksonville Investigation, even if it did not already have those records from the Louisiana Investigation. Her testimony also establishes by a preponderance of the evidence that the FBI would have sought those records *before* it attempted to contact Defendant or obtain the federal search warrant for his Aurora home.

In arguing to the contrary, Defendant insists that the Government cannot rely on the Jacksonville Investigation to establish that it would have conducted a lawful search because the Government knew of and relied upon the Jacksonville Investigation in the Aurora search warrant application. [129] at 4. In other words, Defendant argues, the Jacksonville Investigation information “is distinctly intertwined with the warrants at issue here and cannot be a justification *independent* of the objected to warrants.” *Id.* at 5 (emphasis in original).

⁸ As noted above, this Court finds Agent McDaniel’s testimony (both in-court and via affidavit) to be highly credible.

Defendant's argument improperly conflates the different warrants in this case by referring to them collectively. Here, the alleged impropriety relates to the Louisiana Search Warrant.⁹ This alleged impropriety only taints the subsequent federal search warrants insofar as they might constitute fruit of the poisonous tree. Therefore, removing the Louisiana Search Warrant information from the probable cause analysis for the federal search warrants removes any "nexus sufficient to provide a taint." *United States v. Jones*, 72 F.3d 1324, 1330 (7th Cir. 1995) (quoting *Nix*, 467 U.S. at 443) (holding that if the Government shows that the inevitable discovery doctrine applies, then a court will not exclude any "evidence that eventually would have been located had there been no error.").

Clearly, the Government cannot rely upon information derived from the Louisiana Search Warrant to meet its burden on inevitable discovery, but the same does not hold true for information from the Jacksonville Investigation. The Jacksonville Investigation did not derive from the Louisiana Search Warrant; nor were the two "inextricably intertwined" as Defendant claims. Instead, the two sources developed totally independently. That the affidavit for the federal search warrant of Defendant's Aurora home relied upon both the Jacksonville Investigation and the Louisiana Investigation (because they both supported probable cause) is irrelevant and fails to undermine the independent nature of the two separate underlying investigations. In other words, the fact that the two independent

⁹ In a supplemental reply, which the Court permitted, Defendant also complains that the FBI Buffalo Field Office illegally obtained his mobile device IP address information. The Court takes this issue up in the next section.

investigations later came together in reality, says nothing about what would have happened inevitably in the absence of one of them.

In sum, the Government established that the inevitable discovery doctrine applies to both the records obtained from the Louisiana Search Warrant and the evidence obtained from the subsequent federal search warrants, including Defendant's statements to FBI agents.

B. The Verizon Subpoena and the Fourth Amendment

In his supplemental reply [133] filed after the Government raised the inevitable discovery doctrine, Defendant argues that the FBI Buffalo Field Office also violated his Fourth Amendment rights when it obtained the IP address logs for his mobile phone from Verizon without a warrant. [133].

As discussed above, after Jacksonville referred its investigation to the FBI Buffalo Field Office, an FBI agent subpoenaed Verizon for the IP address logs for the mobile phone number associated with the @davidbanks1014 Musical.ly account for May 6–7, 2017 (the dates the Jacksonville minors received the Musical.ly messages) and July 24, 2017 (a date close to the subpoena request). Verizon returned the IP addresses associated with that mobile number on those dates, and, using a publicly accessible IP geolocation website, the agent identified them as dynamic IP addresses likely linked to the general Chicagoland area.

Defendant argues that the Government needed a court order supported by probable cause to obtain these IP address logs. *Id.* He also insists that the FBI “predicated its entire investigation” on this illegally obtained IP address information because it provided the link to Chicago, and therefore it provided the probable cause

to search Defendant's Aurora home. [133] at 1, 6. Consequently, Defendant argues, this Court must quash the Aurora search warrant and suppress any evidence derived from it. [133], [141].

To begin, Defendant fails to explain how the FBI purportedly “predicated its entire investigation” on this IP address information, and the factual record does not otherwise support that assertion. Instead, as discussed above, the federal search warrant application for Defendant's Aurora home relied upon many facts; and other independent lines of inquiry (flowing from the Jacksonville Investigation, in particular) linked Defendant to the Chicago area and Aurora, specifically. Perhaps Defendant believes that any reliance on the IP address information automatically invalidates the Aurora search warrant application—but he does not explain why. Or perhaps Defendant means to argue that this somehow defeats the Government's inevitable discovery theory. But again, he does not articulate how it does so and, for this reason alone, Defendant fails to establish a basis to quash any warrant or suppress evidence derived from it. *United States v. Butler*, 58 F.4th 364 (7th Cir. 2023) (holding that a party waives perfunctory or undeveloped arguments). Nevertheless, even if Defendant had properly articulated a theory, his motion still fails because he cannot establish that the IP address subpoena constituted an unlawful search under the Fourth Amendment.

The law provides two paths to determine if something constitutes a Fourth Amendment search or seizure. First, a property-based approach draws from common-law trespass and considers whether officers obtained “information by physically

intruding on a constitutionally protected area.” *United States v. Jones*, 565 U.S. 400, 405 (2012). Second, a privacy-based approach, derived from Justice Harlan’s concurrence in *Katz v. United States* considers whether a person has an actual (*i.e.*, subjective) expectation of privacy in the information or material searched “that society is prepared to recognize as reasonable.” 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

Using either path, a court draws from “historical understandings ‘of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted’” to inform its analysis, including in deciding under the Justice Harlan standard whether a “subjective expectation of privacy” is objectively reasonable. *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018) (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)). The party seeking suppression “bears the burden of establishing that he had a reasonable expectation of privacy in what was searched.” *United States v. Tuggle*, 4 F.4th 505, 513 (7th Cir. 2021) (quoting *United State v. Scott*, 731 F.3d 659, 663 (7th Cir. 2013)).

To establish a reasonable expectation of privacy in his mobile device IP address information, Defendant relies upon the Supreme Court’s decision in *Carpenter*, 138 S. Ct. at 2206. There, the Government obtained a court order under the Stored Communications Act to collect 127 days of historical cell-site location information (CSLI) for a robbery suspect’s cell phone number. *Id.* at 2212–13.¹⁰ The CSLI

¹⁰ To obtain such an order, the Government does not need to show probable cause, but instead must show “reasonable grounds” to believe that records will prove “relevant and material to an ongoing investigation.” *Carpenter*, 138 S. Ct. at 2212 (quoting 18 U.S.C. § 2703(d)).

provided approximately 101 precise location data points each day for the defendant's cell phone and showed within 50 meters of accuracy the date and time the cell phone mapped to a location. *Id.* at 2213–19. Over defendant's objection, the Government offered this evidence at trial to place the defendant's cell phone in the vicinity of four armed robberies, and a jury convicted the defendant of all but one firearm count. *Id.* at 2213.

The Supreme Court held that the Government's use of the CSLI records constituted a *de facto* tracking device that invaded the defendant's reasonable expectation of privacy and qualified as a Fourth Amendment search. *Id.* at 2216–20 (citing *Jones*, 565 U.S. at 430 (holding that use of a global-positioning satellite device to track a vehicle's movements in public areas constitutes a search under the Fourth Amendment)). It also found that the CSLI implicated unique and serious privacy interests because those records divulged, on a retroactive basis, “an all-encompassing record of the holder's whereabouts,” providing “an intimate window into” his “life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’” *Id.* at 2217 (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)).

The Government in *Carpenter* had argued that the defendant willingly shared the CSLI with the cellular company when he used the phone, so he possessed no reasonable expectation of privacy in it under the third-party doctrine. This doctrine derives from two cases: *United States v. Miller*, 425 U.S. 435, 443 (1976), where the Court found no reasonable expectation of privacy in banking records; and *Smith v.*

Maryland, 442 U.S. 735, 740 (1979), where the Court found no reasonable expectation of privacy in landline telephone records maintained by a telephone company. In both cases, the Court held that by voluntarily conveying the information to a third-party company, the defendants “‘assumed the risk’ that the company’s records ‘would be divulged to the police.’” *Carpenter*, 138 S. Ct. at 2216 (quoting *Smith*, 442 U.S. at 745).

The *Carpenter* Court reaffirmed the vitality of the third-party doctrine but found that it did not apply to the CSLI records. It held that, unlike bank transactions and phone calls, which require affirmative acts, a cellular phone automatically generates detailed location data (CSLI records) “without any affirmative act on the part of the user beyond powering up.” *Id.* at 2220. Further, the Court emphasized that *Miller* and *Smith* did “not rely solely on the act of sharing,” but also focused both on the nature of the privacy and level of detail the information contained, finding that the bank records in *Miller* related to commercial transactions rather than confidential communications; and the telephone logs in *Smith* revealed too little “identifying information.” *Carpenter*, 138 S. Ct. at 2219 (citing and quoting *Miller*, 425 U.S. at 442 and *Smith*, 442 U.S. at 742). In contrast, the Court held, the nature of CSLI presents considerable privacy concerns because it provides a “detailed chronicle of a person’s physical presence compiled every day, every moment.” *Id.* The Court also reasoned that because carrying a cell phone has become “indispensable to participation in modern society,” one does not voluntarily assume “the risk of turning

over a comprehensive dossier of his physical movements” simply by carrying one. *Id.* (citing *Smith*, 442 U.S. at 745).

In so finding, the Court agreed that the CSLI records captured movements in many public areas, and that law enforcement may, of course, pursue a suspect in public “for a brief stretch.” *Id.* at 2217. It held, however, that a “person does not surrender all Fourth Amendment protection by venturing into the public sphere”; rather, the law recognizes “society’s expectation” that the Government “would not—and indeed, in the main, simply could not—secretly monitor and catalogue” an individual’s every movement “for a very long period” without court authorization. *Id.* (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring)).

Here, Defendant argues that the dynamic IP address information that the FBI Buffalo Field Office obtained for his mobile device remains the functional equivalent of the CSLI records in *Carpenter*. He maintains that, like CSLI records, dynamic IP addresses “reveal day-to-day information about the owner’s whereabouts” and “these records are effortlessly compiled” by wireless carriers. [133] at 6. He also claims that a mobile device user does not make a meaningful choice to share dynamic IP address information; instead “IP addresses are logged whenever a cell phone accesses the internet in the background to search for software updates, send and receive messages, sync to a time zone, and update the weather forecast, just to name a few.” [133] at 7.

In response, [136], the Government points to *United States v. Soybel*, 3 F.4th 584 (7th Cir. 2021), which found that the third-party doctrine applied to IP address information that the FBI gathered by installing a pen register at the defendant’s

apartment complex. *Id.* at 586, 588. Through this pen register, the FBI tracked internet activity flowing in and out of the defendant's apartment complex for sixty days and linked his unit to ongoing cyberattacks on his former employer.

In finding no reasonable expectation of privacy in *Soybel*, the Seventh Circuit held that the defendant assumed the risk of disclosure when he voluntarily communicated with third parties by using the internet. *Id.* at 593–94. It also rejected the defendant's reliance on *Carpenter*, emphasizing that “*Carpenter* was ‘novel’ both as to the instrumentality of the search and in the information captured” because CSLI gives “an all-encompassing record of the holder's whereabouts,” presenting serious privacy concerns magnified by the data's retrospective quality, which gave “police access to a category of information otherwise unknowable.” *Id.* at 592 (quoting *Carpenter*, 138 S. Ct. at 2217–18). In contrast, it held, the pen register installed in Soybel's building “could not capture the whole of Soybel's physical movements,” only “incidentally revealed when Soybel may have been in his apartment,” and did not have a “retrospective” quality. *Id.* at 593.

The Government argues that *Soybel* controls here because, unlike the CSLI in *Carpenter*, the IP address information here only incidentally divulged the mobile device's geographic location and did so only generally. Moreover, the Government argues that the Defendant voluntarily disclosed this IP address information to Verizon by using the internet, making it subject to the third-party doctrine exception. [136] at 3; *see also United States v. Caira*, 833, F.3d 803, 809 (7th Cir. 2016) (finding that the DEA lawfully used IP address information tied to a defendant's email

account logins to learn his exact home and work locations because defendant had “no reasonable expectation of privacy” in IP addresses information that he “voluntarily shared” with the ISP).

As explained below, this case resembles *Soybel* more than *Carpenter*, and Defendant has failed to establish a reasonable expectation of privacy in the mobile IP address information at issue here.

1. Dynamic Versus Static IP Addresses

First, Defendant tries to distinguish his case from *Soybel* by drawing a distinction between dynamic IP addresses and static IP addresses. [133]. As discussed above, an IP address is a unique series of numbers that an Internet Service Provider (ISP) assigns to a device so it can connect to the internet and exchange information with websites. An ISP may assign a device a “static” or “dynamic” IP address. [145] ¶ 4. If an ISP assigns a static IP address, then the device uses that IP address anytime the device accesses the internet. *Id.* ¶ 5. A dynamic IP address, however, is not permanently assigned to one device, and an ISP may assign it to a device temporarily, and later assign it to a different device. *Id.*

Defendant seems to believe that mobile devices only use dynamic IP addresses while stationary devices always use static IP addresses. As a result, he argues that static IP addresses “do not reveal much personal information beyond a general location or home access,” but the use of dynamic IP addresses by mobile devices will, allegedly, always reveal the owner’s day-to-day movements, providing to the Government on a retroactive basis “an exhaustive chronicle of personal information.”

[133] at 5–7. He also argues that even if one voluntarily shares static IP address information by accessing the internet at home, one does not voluntarily share dynamic IP addresses because, he alleges, mobile devices automatically access the internet and transmit IP address information “without any affirmative act on the user’s part beyond powering up.” [133] at 7 (quoting *Carpenter*, 138 S. Ct. at 2219). Thus, he reasons, *Soybel*’s holding applies to static IP address searches since it involves a defendant’s home internet use, but *Carpenter* should control this Court’s analysis of dynamic IP address data because they involve mobile devices. *Id.*

The factual record does not support the categorical distinction Defendant tries to draw between static and dynamic IP addresses. Instead, Agent McDaniel testified that most devices, whether stationary or mobile, use dynamic IP addresses and ISPs usually reserve static IP addresses for large businesses. Defendant’s own cited source confirms this fact. See Alexander S. Gillis, *Definition: dynamic IP address*, <https://www.techtarget.com/whatis/definition/dynamic-IP-address> (last visited February 9, 2023). Defendant’s cited source also indicates that any device, including a mobile device, may use a “static” IP address if the user has access to one and configures the device to use it. *Id.* Consequently, the constitutional question does not turn upon a purported static-dynamic IP distinction.

Instead, the real issue is whether “mobile device” IP address information warrants different protection than “stationary device” IP address information. Afterall, the *Carpenter* Court highlighted aspects of mobile device CSLI that could pose significant privacy concerns—it provides precise location information; service

providers maintain extensive CSLI, giving the Government an easy retrospective view of a cellphone's exact movements; cellphones constantly generate and transmit CSLI without any real action by the cellphone's user; and cellphones have become nearly essential to modern life. The question is, therefore, has Defendant shown that the same privacy concerns raised in *Carpenter* hold true for mobile device IP address data?

2. Expectation of Privacy in Mobile Device IP Address Information

As Defendant points out, the mobile IP address data here, like the CSLI in *Carpenter*, was retrospective. Likewise, Defendant also argues, and the Government does not dispute, that mobile devices with internet access have become nearly as ubiquitous in modern society as mobile devices with a cellular connection. The similarities stop there, however, at least on the factual record in this case. This proves fatal to Defendant's motion because, as the party seeking suppression, he bears the burden to show that he had a reasonable expectation of privacy in his mobile device IP address information. *Tuggle*, 4 F.4th at 513.

First, Defendant argues that mobile device IP address data reveals a user's precise day-to-day movements, providing "an exhaustive chronicle of personal information." [133] at 5–7. The factual record does not support this claim. Instead, as discussed above, an FBI agent subpoenaed Verizon for the IP address information associated with Defendant's cell phone on the dates the illicit Muscial.ly messages were sent. The Agent then used a publicly available search tool to link those addresses to the Chicagoland area. The parties stipulate that these search tools only

give the “calculated accuracy radius measured in kilometers of the estimated location.” [145] ¶ 6.e. As an example, one publicly available search tool gave location information for the six IP addresses here on a particular day with radius accuracy varying from 100 to 500 kilometers (roughly 60 to 300 miles). *Id.* ¶ 7.

Such broad location information hardly reveals a user’s day-to-day movements; nor does it raise the constitutional concerns present in *Carpenter* or otherwise provide “an exhaustive chronical of personal information” as Defendant argues. Instead, it only revealed that on a particular day Defendant’s cell phone may have been in the Chicagoland area (with likely accuracy within 10s or 100s of miles). Defendant points to no authority holding that a person has a reasonable expectation of privacy in the broad geographic location contained in this type of third-party business record. And *Carpenter* certainly does not hold as much. To the contrary, *Carpenter*’s holding relied upon the Court’s tracking device precedent, 138 S. Ct. at 2217 (citing *Jones*, 565 U.S. at 430), and held that CSLI posed even greater privacy concerns because it gave the Government “near perfect surveillance, as if it had attached an ankle monitor to the phone’s user,” 138 S. Ct. at 2218. The generalized location information here provides nothing of the sort.

Next, Defendant argues that, even if the mobile phone IP address data in this case gives less precise location information than CSLI, the *Carpenter* opinion “is meant to account for sophisticated surveillance in development.” [133] at 6. Defendant insists that location technology linked to IP addresses “is rapidly approaching CSLI-levels of accuracy.” *Id.* In fact, Defendant maintains that “IP

geolocation technology is as accurate as CSLI.” *Id.* at 7. Yet again, he provides no supporting evidence about these purported advances in IP address location technology let alone prove that current IP geolocation technology is, in fact, as precise as CSLI. Indeed, the parties’ stipulations show just the opposite.

Importantly, *Carpenter* emphasized that its decision remained “a narrow one” that did not express a view on matters not before the Court or “call into question conventional surveillance techniques and tools.” 138 S. Ct. at 2220. This Court cannot extend *Carpenter* to cover a different technology based upon a party’s mere speculation about what that technology can do now or, even more dangerously, a party’s unsupported fears about what technology might do in the future. Instead, the Court must make a “fact-specific inquiry” to determine whether a defendant has a reasonable expectation of privacy in the subject of the search at hand. *Burnside*, 588 F.3d at 517. And, Defendant, as the party seeking suppression here, bears the burden to show he had a reasonable expectation of privacy in the IP address information at issue. *See Tuggle*, 4 F.4th at 513. He has not met his burden.¹¹

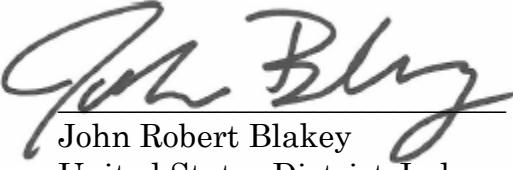
¹¹ *Soybel* also relied upon the third-party doctrine in denying the defense request for suppression and noted, among other factors, that the disputed device generated IP address information when someone chose to use the internet. 3 F.4th at 593–94; *see also Caira*, 833 F.3d at 806 (applying third party doctrine to find no reasonable expectation of privacy in IP addresses tied to defendant’s email account). Here, the Government also asserts that the ISP only generates mobile device IP address information when the user purposely accesses the internet on a mobile device. In contrast, Defendant argues—again without factual support—that a mobile device periodically accesses the internet without any action by a user, and that one can only stop these default functions by turning a phone to “airplane mode”, disconnecting wi-fi, or otherwise disabling a phone’s core functions. [133] at 7. The Court need not resolve this gap in the factual record, however, because Defendant failed to otherwise establish a reasonable expectation of privacy in the general geographic location of the IP address information generated by his mobile device.

III. Conclusion

Based upon the above, the Court denies Defendant's Motion to Quash Search Warrants and Suppress Evidence Seized [110].

Date: February 10, 2023

ENTERED:



John Robert Blakey
United States District Judge